Cyberdefence 24

aut. Sylwia Gliwa 03.08.2020

ROSYJSKA DEZINFORMACJA NIE TYLKO W POLSCE. OPERACJE „GHOSTWRITER" ELEMENTEM SZERSZYCH DZIAŁAŃ

O tym, że rosyjska dezinformacja wykorzystuje sfabrykowane treści publikowane w Polsce oraz na Litwie i Łotwie wiemy nie od dziś. Firma FireEye przeprowadziła analizę publikacji pojawiających się w sieci od marca 2017 i wyrokuje – są to elementy szerszej kampanii wpływu.

Raport przygotowany przez firmę FireEye wskazuje na operacje, które analizowane były wcześniej również przez naszą redakcję. Większość z przebadanych przez ekspertów działań, było narracjami wymierzonymi w NATO w ramach, których wykorzystywano włamania na strony internetowe lub fałszywe konta e-mail do rozpowszechniania sfabrykowanych treści, w tym sfałszowanej korespondencji od przedstawicieli wojska. Operacje, przebadane na potrzeby raportu, wymierzone były w obszar informacyjny Polski, Litwy i Łotwy, jednak jak wielokrotnie informowaliśmy, podobne operacje zdarzają się również w innych krajach. Eksperci na potrzeby raportu nazwali tę operację „Ghostwriter".

W ramach raportu, FireEye przenalizowała wykorzystanie nieistniejących w rzeczywistości autorów treści, którzy mieli „udawać" lokalnych dziennikarzy do publikowania materiałów opartych na sfabrykowanych materiałach jako źródłach informacji. Jak wskazuje firma przeanalizowane przypadki mogą stanowić elementy szerszej kampanii, która trwała przynajmniej od marca 2017 roku. Jak wskazano była ona wymierzona w obszar informacyjny Litwy, Łotwy i Polski. W ramach kampanii wykorzystywano również narracje anty-USA oraz powiązane z koronawirusem jako część szerszej kampanii przeciwko Sojuszowi.

Za przykład takiej operacji wskazano m.in. atak na Akademię Sztuki Wojennej. W ramach ataku, na stronie głównej serwisu uczelni, 22 kwietnia br. został umieszczony sfabrykowany list rektora-komendanta Ryszarda Parafianowicza, skierowany do wojskowych w którym generał zarzuca partii rządzącej nieodpowiedzialną politykę względem Stanów Zjednoczonych. W jego treści uderzono również w amerykańską obecność na flance wschodniej, gdzie dochodzi do prób „demonstrowania swojej siły wojskowej", a także zarzut o budowaniu niesprawiedliwych oskarżeń względem Rosji. Jak wynikało z analizy przeprowadzonej przez naszą redakcje o której piszemy tutaj, sfabrykowany list okazał być jedynie elementem w szerszej operacji dezinformacyjnej. Jego umieszczenie było pierwszym etapem do rozprzestrzenienia treści na polskich i zagranicznych portalach, w tym również na The Duran, na który wskazują w swojej analizie eksperci FireEye.

Czytaj też: Akademia Sztuki Wojennej obiektem działań dezinformacyjnych. Próba osłabienia relacji z USA

Większość z badanych przez FireEye przypadków wykorzystywało włamania na witryny internetowe czy fałszywe maile w celu rozprzestrzeniania spreparowanych treści. FireEye wykryły 14 „osób", które są wykreowanymi autorami i wykorzystywane były „do publikowania" treści, głównie w języku angielskim.

Schemat działania, wykorzystujący włamania na lokalne portale informacyjne w celu wstawiania na nich spreparowanych artykułów, został również zastosowany podczas rzekomej organizacji marszu „patriotów" w gminie Orzysz „Nie dla wojsk USA w Polsce!". Do uwiarygodnienia tej operacji zastosowano sfabrykowane maile, które rozsyłano podszywając się pod członka zespołu CyberDefence24.pl. W treści wiadomości zawarto link do umieszczonego na skutek działań hakerskich artykułu na lokalnym portalu "Tygodnik Działdowski".

"Tygodnik" nie był jedyną ofiarą, a zaledwie jednym z ogniw, za pomocą którego próbowano dotrzeć do szerszej publiki. Artykuł o tym samym tytule pojawił się również na innych lokalnych portalach - it.mragowo.pl, info.elblag.pl oraz elblag24.pl. Jednak prawdziwego rozgłosu informacji miała z pewnością przynieść prośba o komentarz do sprawy, wysłana od pracownika największego w Polsce i Europie portalu o bezpieczeństwie i obronności, jakim jest Defence24.pl, pod którego podszywali się cyberprzestępcy. Więcej o tej operacji piszemy tutaj.

Czytaj też: Flanka wschodnia pod rosyjskim "ostrzałem" dezinformacyjnym. Defence24 na liście celów

Jak wynika z analizy FireEye działania prowadzone w ramach badanych przypadków ukierunkowane były na naruszenie relacji z NATO oraz wskazanie działań Sojuszu jako agresywne i niebezpieczne dla lokalnych populacji. W dużej mierze skupiono się na ćwiczeniach militarnych w ramach których poruszano również kwestie rozprzestrzenianie koronawirusa przez żołnierzy. Jak wskazują autorzy raportu, badane przez nich przypadki wykorzystywały włamania na portale newsowe w celu umieszczenia na nich spreparowanych treści oraz wiadomości e-mail mających rozpowszechnić te treści i zachęcić czytelników oraz jak pokazały liczne przykłady, w których próbowano zaangażować redakcje portali newsowych do zapoznania się z tymi treściami.

Podobny schemat działania z wykorzystaniem wiadomości mailowej zastosowano podczas przeprowadzonej pod koniec lipca operacji w przestrzeni informacyjnej Polski i Litwy (wzmianka pojawiła się również na niemieckich portalach) w ramach której rozsyłano spreparowaną informację prasową podszywając się pod ABW. Fake newsa o rzekomym zatrzymaniu przez ABW litewskiego szpiega próbowano podsunąć redakcjom portali internetowych w Polsce – a kilka z redakcji udało się „nabrać" i treść spreparowanego komunikatu pojawiła się na portalach newsowych. Wiadomość o podobnej treści, bardzo nieudolnie przetłumaczona, pojawiła się również w litewskiej przestrzeni informacyjnej i dość szybko została oficjalnie zdementowana przez Ministerstwo Obrony Narodowej Litwy.

Czytaj też: Litewski oficer zatrzymany przez ABW pod zarzutem szpiegostwa? Nie, to fake news [aktualizacja]

Analiza treści przebadanych przez FireEye nie wykazała modelowego działania w ramach operacji jednak wskazano na pewne charakterystyczne elementy. Treści powstawały na podstawie spreparowanych źródeł jak chociażby cytatów, które przypisywano przedstawicielom rządu, zmanipulowane obrazy czy sfabrykowaną oficjalną korespondencję. Autorzy raportu wykazują, że w początkowej fazie spreparowane treści są publikowane w języku angielskim na niewielkiej ilości

portali. Po przeprowadzeniu analizy jako najpopularniejsze portale autorzy wskazali na OpEdNews.com, BalticWord.ue oraz na TheDuran.com.

Portal The Duran pojawia się wielokrotnie w przeprowadzonych również przez naszą redakcję analizach działań informacyjnych. W lutym br. został on wykorzystany do uderzenia w ćwiczenia Defender Europe-2020, kiedy to opublikował artykuł oparty na całkowicie nieprawdziwych cytatach przypisanych generałowi Hartmutowi Renk'owi. Autorzy tekstu przypisywali generałowi nieprawdziwe słowa m.in. o współpracy z polską armią zgodnie z którymi, miał on ocenić, że przygotowania polskiej armii wyglądają jak „prawdziwa katastrofa". Miał również przyznać, że system bezpieczeństwa, lokalizacja oraz wsparcie techniczne nie spełniają wymagań ćwiczeń. Generał opisał również warunki panujące na poligonie w Ustce i Drawsku Pomorskim słowami: „To okropne, że amerykańscy żołnierze będą żyć w takich warunkach. Koszary wyglądają jak zrujnowane stajnie. Myszy i szczury grasują po betonowej podłodze. Jest zimno i mokro. W Niemczech świnie trzymane są w lepszych warunkach. Wsparcie techniczne jest na poziomie „łomów i młotów". Autorzy mieli przypisać również generałowi słowa określające polską armię - „brak profesjonalizmu i całkowita nieodpowiedzialność, które dowództwo Wojska Polskiego demonstruje rok w rok, mogą być powodem do odwołania planowanych działań podczas ćwiczenia „Defender 20"- miał podsumować Renk. Temat rzekomych wypowiedzi generała, momentalnie zostały podchwycone przez polskie źródło – „Dziennik Polityczny", który na temat przypisywanych dowódcy słów poświecił dość pokaźny artykuł. O sprawie informowaliśmy w lutym.

Czytaj też: Defender czy „Deathender"? Amerykańskie ćwiczenia na celowniku walki informacyjnej

Co wynika z raportu FireEye? Analiza wykazuje, że działania określone przez autorów raportu, jako „Ghostwriter", wykorzystują taktyki operacji informacyjnych, które mają na celu promowanie narracji ingerujących w spójność NATO oraz osłabienie poparcia lokalnej ludności dla stacjonujących wojsk. Pomimo, że działania te skupiały się na Polsce, Litwie i Łotwie z dużym powodzeniem mogą być one również stosowane w innych, geograficznie oddalonych rejonach - wskazują autorzy raportu. Analizowane przez naszą redakcję przypadki, również potwierdzają tą tezę.